Die Existenz eines ungeraden quadratischen Nichtrestes mod p im Intervall $1, \sqrt{p}$.

Von L. RÉDEI in Szeged.

Bezeichne p eine ungerade Primzahl und $[x]$ die größte ganze Zahl $\leqq x$. Eine der schönsten Tatsachen in der Theorie der Verteilung der quadratischen Reste ist der folgende Satz von VINOGRADOV [7][1]):

Unter irgendwelchen $3[\sqrt{p}]-1$ *aufeinanderfolgenden ganzen Zahlen gibt es (mindestens) einen quadratischen Nichtrest* mod p.

Insbesondere folgt aus diesem Satz, daß es für $p>23$ im Intervall $1, 3[\sqrt{p}]$ einen quadratischen Nichtrest mod p gibt. Diesen speziellen Satz haben wir [4] in zwei Richtungen verschärft, indem wir in einem kürzeren (ebenfalls mit 1 beginnenden) Intervall die Dichtigkeit der quadratischen Nichtreste mod p bestimmt haben. Und zwar gilt:

Im Fall $p\equiv 1 \pmod 4$ enthält das Intervall $1, [\sqrt{p}]$ mindestens

$$\frac{[\sqrt{p}]}{4+2\sqrt{2}}\left(>\frac{[\sqrt{p}]}{7}\right)$$

quadratische Nichtreste mod p. Im Fall $p\equiv -1 \pmod 4$ enthält das Intervall $1, \left[2\sqrt{\frac{p}{3}}\right]$ mindestens

$$\frac{\left[2\sqrt{\frac{p}{3}}\right]}{8+4\sqrt{3}}\left(>\frac{\left[2\sqrt{\frac{p}{3}}\right]}{15}\right)$$

quadratische Nichtreste mod p.

Neulich hat NAGELL [1], [2] das Problem des kleinsten positiven ungeraden [2]) quadratischen Nichtrestes mod p untersucht. Nach ihm gilt folgendes:

Ist $p\equiv 1 \pmod 8$ oder $p\equiv 7 \pmod 8$, $p\neq 7, 23$, so gibt es eine ungerade Primzahl $q<\sqrt{p}$ mit $\left(\frac{q}{p}\right)=-1$.[3]) Ist $p\equiv 3 \pmod 8$ oder $p\equiv 5 \pmod 8$, so gilt ähnliches für $2\sqrt{p}+1$ bzw. $\sqrt{2p}$ statt $\sqrt{p}$.

---

[1]) Mit [ ] wird auf das Literaturverzeichnis am Ende unserer Arbeit hingewiesen.

[2]) Das Wort „ungerade" ist in den Fällen $p\equiv 1, 7 \pmod 8$ überflüßig, in den Fällen $p\equiv 3, 5 \pmod 8$ dagegen wesentlich.

[3]) Der auf $p\equiv 1 \pmod 8$ bezügliche Teil ist eine Folgerung aus unserem obigen Satz.

Wir verschärfen NAGELLs Satz wie folgt:

Satz. *Für jede ungerade Primzahl*

(1) $$p \neq 3, 5, 7, 11, 13, 23, 59, 109, 131$$

gibt es eine ungerade Primzahl $q < \sqrt{p}$ *mit* $\left(\frac{q}{p}\right) = -1$.

Die Fälle $p \equiv 1, 7 \pmod 8$ hat NAGELL mit Hilfe des folgenden Satzes von THUE bewiesen (s. SCHOLZ [6]):[4])

Für jede positive Primzahl p lassen sich alle primen Restklassen mod p durch die Zahlen

$$\pm\frac{x}{y} \qquad (x, y = 1, 2, \ldots < \sqrt{p}; \quad (x, y) = 1)$$

repräsentieren.

Die anderen zwei, weit schwierigeren Fälle $p \equiv 3, 5 \pmod 8$ des Satzes ließen sich dagegen wegen $\left(\frac{2}{p}\right) = -1$ aus THUEs Satz kaum gewinnen.

Vollständigkeitshalber beweisen wir den Satz im ganzen Umfange, wobei wir den auch von NAGELL [2] erledigten Fall $p \equiv 7 \pmod 8$ kürzer und ohne Anwendung des Satzes von Thue beweisen werden.

Vor allem läßt sich leicht nachprüfen, daß die neun Primzahlen auf der rechten Seite von (1) wirkliche Ausnahmefälle sind. Im folgenden werde (1) schon angenommen. Wir bezeichnen mit e die größte ganze Zahl $< \sqrt{p}$, wofür also

(2) $$0 < p - e^2 < 2e$$

gilt. Gleich bemerken wir, daß wegen (1)

(3) $$e \geqq 4$$

ist. Es genügt zu zeigen, daß es unter den ungeraden Zahlen

(4) $$1, 3, 5, \ldots, \quad (\leqq e)$$

einen quadratischen Nichtrest mod p gibt, denn eine solche Zahl hat mindestens einen Primfaktor, der ebenfalls quadratischer Nichtrest mod p ist.

Fall $p \equiv 1 \pmod 8$.

Da jetzt $\left(\frac{-1}{p}\right) = 1$ ist, so folgt aus THUEs Satz, daß es unter den Zahlen $\frac{x}{y} y^2 = xy$ $(x, y = 1, 2, \ldots, e)$, also auch unter den

(5) $$1, 2, \ldots, e$$

[4]) Für eine weitgehende Verallgemeinerung des Thueschen Satzes siehe RÉDEI [3]. Anwendungen finden sich bei RÉDEI [4], [5].

einen quadratischen Nichtrest mod p geben muß. Da ferner jetzt $\left(\frac{2}{p}\right)=1$ gilt, so folgt ähnliches für die Zahlen (4), womit der Satz für diesen Fall bewiesen ist.

In den übrigen Fällen beweisen wir den Satz am bequemsten unter der Annahme, daß alle Zahlen (4) quadratische Reste mod p sind. Unser Beweisverfahren wird sein, daß wir trotzdem einen quadratischen Nichtrest mod p angeben, der eine der Zahlen (4) ist.

Fall $p\equiv 7 \pmod 8$.

Mit P, Q bezeichen wir zwei solche Zahlen, die gleich einem Produkt von je zwei Zahlen aus (5) sind. Es genügt die Existenz eines Paars P, Q mit $P+Q=p$ auszuweisen, denn dann muß wegen $\left(\frac{-1}{p}\right)=-1$ entweder $\left(\frac{P}{p}\right)=-1$ oder $\left(\frac{Q}{p}\right)=-1$ gelten, woraus wegen $\left(\frac{2}{p}\right)=1$ der gewünschte Widerspruch folgt. Wir unterscheiden die folgenden Fälle:

Fall $2\nmid e$. Wegen (2) ist $P=e^2$, $Q=2\frac{p-e^2}{2}$ ein gewünschtes Paar. Für den übriggebliebenen Fall $2\mid e$ bemerken wir gleich, daß dann gewiß

$$e\geqq 8$$

ist. Im anderen Falle wäre nämlich nach (3) entweder $e=4$, $p=23$, was aber wegen (1) falsch ist, oder $e=6, p=47$, was wegen $\left(\frac{5}{47}\right)=-1$ ebenfalls widersprüchig ist.

Fall $2\mid e$, $8\mid p-(e-1)(e-3)$. Ein geeignetes Paar ist

$$P=(e-1)(e-3),\quad Q=8\frac{p-P}{8},$$

da der letzte Faktor ganz und nach (2)

$$\leqq\frac{1}{8}(6e-3)<e$$

ist.

Fall $2\mid e$, $8\nmid p-(e-1)(e-3)$. Hieraus folgt

$$8\mid p-(e-3)(e-5). \tag{6}$$

Wenn sogar

$$16\mid p-(e-3)(e-5) \tag{7}$$

gilt, so ist

$$P=(e-3)(e-5),\quad Q=16\frac{p-P}{16}$$

ein passendes Paar, da nach (2) der letzte Faktor

$$\leqq \frac{1}{16}(10e-15) < e$$

ist.

Wenn dagegen (7) falsch ist, so gilt wegen (6)

$$16 \mid p-(e-1)(e-7),$$

somit is jetzt

$$P=(e-1)(e-7),\quad Q=16\frac{p-P}{16}$$

ein passendes Paar, da der letzte Faktor $< e$ ist.

Fall $p \equiv 3 \pmod 8$.

Es genügt, wenn wir eine ungerade ganze Zahl N mit $0 < N \leqq e$ angeben, wofür $\left(\frac{N}{p}\right) = -1$ gilt. Hierzu werden wir weitere Fälle unterscheiden müssen. In jedem Fall werden wir N in der Form

$$N=\frac{uv-p}{2^{2k+1}3^l} \text{ oder } N=\frac{p-uv}{2^{2k+3}3^l}$$

mit $k, l = 0, 1$ und

$$u, v = 1, 3, 5, \ldots$$

angeben, wobei wir stets darauf achten, daß die an N gestellten Forderungen erfüllt sind. Insbesondere sichern wir die Erfüllung von $\left(\frac{N}{p}\right) = -1$ wegen $\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=-1$, $\left(\frac{3}{p}\right)=1$ so, daß wir u, v durch $\left(\frac{u}{p}\right)=\left(\frac{v}{p}\right)$ einschränken. Hierzu genügt es, wenn wir auch noch für

$$u=v \text{ oder } u, v \leqq e \text{ oder } u \leqq e, v \leqq 3e, 3 \mid v$$

sorgen, denn dann wird in den zwei letzteren Fällen wegen der Annahme über (4) sogar $\left(\frac{u}{p}\right)=\left(\frac{v}{p}\right)=1$.

Fall $2 \mid e$. Offenbar ist

$$N=\frac{(e+1)^2-p}{2}$$

eine passende Zahl.

Fall $4 \mid e-1$. Jetzt ist

$$N=\frac{p-e(e-2)}{4}$$

eine passende Zahl.

Es ist nur noch der Fall $4 \mid e+1$ übrig.

Fall $4 \mid e+1$, $3 \mid e$. Vorläufig nehmen wir

$$e > 18 \tag{8}$$

an. Wir betrachten die zwei ganzen Zahlen

$$a = \frac{e(e+6)-p}{8}, \quad b = \frac{(e-6)(e+12)-p}{8}.$$

Es gilt

$$a = b+9,$$

weshalb das eine von a, b ungerade ist. Beide liegen zwischen 0 und e, denn aus (2), (8) folgt

$$b > \frac{1}{8}(4e-72) > 0, \quad a < \frac{6e}{8} < e.$$

Folglich ist jetzt a oder b eine passende Zahl N.

Wenn nun (8) nicht gilt, so kommt wegen (3) nur $e = 15$, d. h. $p = 227, 251$ in Betracht. Auch diese Fälle scheiden aus, da $\left(\frac{5}{227}\right) = -1$, $\left(\frac{11}{251}\right) = -1$ ist.

Fall $4 \mid e+1$, $3 \mid e-1$. Vorläufig nehmen wir

$$e > 40 \tag{9}$$

an. Wir betrachten die vier Zahlen

$$a = \frac{p-(e-4)(e+2)}{16}, \quad b = \frac{p-(e-12)(e+2)}{16},$$

$$c = \frac{p-(e-22)(e+20)}{16}, \quad d = \frac{p-(e-16)(e+14)}{16}.$$

Der Zähler von a ist durch 8 teilbar. Ferner gilt

$$b = a + \frac{e+1}{2} + \frac{1}{2}, \quad c = a+27, \quad d = a+13+\frac{1}{2},$$

Hieraus folgt, $\left(\text{wegen } 2 \left| \frac{e+1}{2} \right.\right)$, daß eine der Zahlen a, b, c, d eine ungerade ganze Zahl ist. Diese ist eine passende Zahl N, insofern sie zwischen 0 und e liegt. Die kleinste der Zahlen a, b, c, d ist a, die größte ist b oder c. Nun gilt nach (2), (9) in der Tat

$$a > \frac{1}{16}(2e+8) > 0,$$

$$b < \frac{1}{16}(12e+24) < e,$$

$$c < \frac{1}{16}(4e+440) < e.$$

Wenn (9) nicht gilt, so kommen nur $e = 7, 19, 31$, d. h. $p = 59, 379, 971, 1019$ in Betracht. Hiervon ist $p = 59$ wegen (1) unmöglich. Auch die

übrigen Fälle scheiden wegen

$$\left(\frac{3}{379}\right)=\left(\frac{11}{971}\right)=\left(\frac{7}{1019}\right)=-1$$

aus.

Fall $4 \nmid e+1$, $3 \mid e+1$. Vorläufig nehmen wir

(10) $$e>30$$

an. Wir betrachten die vier Zahlen

$$a=\frac{p-(e-30)(e-4)}{48}, \quad b=\frac{p-(e-22)(e-10)}{48},$$

$$c=\frac{p-(e-18)(e-16)}{48}, \quad d=\frac{p-(e-12)(e-22)}{48}.$$

Der Zähler von a ist (wegen $p\equiv 2 \pmod 3$) durch 24 teilbar. Ferner gilt

$$b=a-3+\frac{1}{2}, \quad c=a-4+\frac{1}{2}, \quad d=a-3.$$

Hieraus folgt, daß eine der Zahlen a, b, c, d eine ungerade ganze Zahl ist. Diese ist dann eine passende Zahl N, insofern sie zwischen 0 und e liegt. Das ist wegen (10) und (2) in der Tat der Fall, da nach (2)

$$a<\frac{1}{48}(36e-120)<e$$

gilt.

Wenn endlich (10) falsch ist, so kommen nur $e=11, 23$, d. h. $p=131$, 139, 547, 563, 571 in Betracht. Hiervon ist $p=131$ wegen (1) unmöglich. Auch die übrigen Fälle scheiden wegen

$$\left(\frac{3}{139}\right)=\left(\frac{3}{547}\right)=\left(\frac{5}{563}\right)=\left(\frac{3}{571}\right)=-1$$

aus.

Fall $p\equiv 5 \pmod 8$.

In diesem Fall genügt wegen $\left(\frac{-1}{p}\right)=-1$ eine ungerade ganze Zahl N mit $-e\leqq N\leqq e$ und $\left(\frac{N}{p}\right)=-1$ anzugeben. Sonst wird dieser Fall dem vorigen ähnlich, mit der Vereinfachnung, daß wir jetzt ein N in der Form

$$N=\frac{p-uv}{2^{2k+1}}$$

angeben werden können, wobei k, u, v dasselbe bedeuten wie vorher.

Fall $2 \nmid e$, $3 \mid e$. Zunächst sei

(11) $$e>10.$$

Jetzt ist

$$N=\frac{p-(e-4)(e+6)}{2}$$

eine passende Zahl, insofern $-e\leqq N\leqq e$ gilt. Aus (2) folgt in der Tat

$$N>\frac{1}{2}(-2e+24)>-e,$$

$$N<12, N\leqq 11\leqq e.$$

Gilt (11) nicht, so kommt wegen (3) nur $e=9$ in Betracht, dieser Fall fällt aber aus, da zwischen 81 und 100 kein $p\equiv 5 \pmod{24}$ liegt.

Fall $2\nmid e$, $3\mid e-1$. Eine passende Zahl ist

$$N=\frac{p-e(e+2)}{2}.$$

Fall $2\nmid e$, $3\mid e+1$. Jetzt paßt

$$N=\frac{p-(e-2)(e+4)}{2},$$

da nach (2), (3)

$$N>\frac{1}{2}(-2e+8)>-e,$$

$$N<4\leqq e$$

gilt.

Fall $2\mid e$, $3\mid e$. Eine gewünschte Zahl ist

$$N=\frac{p-(e-3)(e+3)}{2},$$

wenn auch $-e\leqq N\leqq e$ gilt. Hiervon ist $N\geqq -e$ trivial. Wenn $N\leqq e$ falsch ist, so gilt $N\geqq e+1$, also

$$p\geqq e^2+2e-7.$$

Wegen (2) und $p\equiv 5 \pmod 8$ müßte $p=e^2+2e-3$ sein, aber die rechte Seite läßt sich in $(e-1)(e+3)$ zerlegen, kann also keine Primzahl sein.

Fall $2\mid e$, $3\mid e+1$. Jetzt paßt

$$N=\frac{p-(e-1)(e+1)}{2}$$

offenbar.

Fall $2\mid e$, $3\mid e-1$. Vorläufig sei

(13) $$e>15.$$

Wir betrachten

$$a=\frac{p-(e-7)(e+5)}{8},\quad b=\frac{p-(e-11)(e+17)}{8}.$$

Beide sind ganz und wegen

$$b = a - e + 19$$

ist das eine von ihnen ungerade, also ein passendes N, vorausgesetzt, daß sie zwischen $-e$ und e liegen. Das trifft zu, da nach (2), (13)

$$a > 0, \quad b > -e.$$

$$a < \frac{1}{8}(4e + 35) < e, \quad b < \frac{1}{8}(-4e + 187) < e$$

ist.

Ist (12) falsch, so kommen nur $e = 4, 10$, also $p = 101, 109$ in Betracht. Wegen (1) ist $p = 109$ unmöglich, auch $p = 101$ scheidet wegen $\left(\frac{3}{101}\right) = -1$ aus. Den Satz haben wir bewiesen.

Anmerkung bei der Korrektur (10. Juni 1953). Vgl. noch die folgenden zwei Arbeiten, in denen ein Teil obigen Satzes, teils in schärferer Form, mit anderer Methode bewiesen wird: T. Nagell, Sur le plus petit non-reste quadratique impair, *Arkiv för Mat.*, **1** (1951), Nr 38; A. Brauer, Über den kleinsten quadratischen Nichtrest, *Math. Zeitschrift*, **33** (1931), 161—176.

Literaturverzeichnis

[1] T. Nagell, Sur les restes et les non-restes quadratiques suivant un module premier, *Arkiv för Mat.*, **1** (1950), Nr 16.
[2] T. Nagell, Sur un théorème d'Axel Thue, *Arkiv för Mat.*, **1** (1951), Nr 33.
[3] L. Rédei, Endlich-projektivgeometrisches Analogon des Minkowskischen Fundamentalsatzes, *Acta Math.*, **84** (1950), 155—158.
[4] L. Rédei, Über die Anzahl der Potenzreste mod p im Intervall $1, \sqrt{p}$, *Nieuw Archief voor Wiskunde*, **23** (1950), 150—162.
[5] L. Rédei, Über eine Verschärfung eines zahlentheoretischen Satzes von Thue, *Acta Math. Acad. Sci. Hung.*, **2** (1951), 75—82.
[6] Scholz, *Einführung in die Zahlentheorie* (Berlin, 1939), insb. S. 45—46.
[7] У. М. Виноградов, Основы теории чисель (I. M. Vinogradov, *Die Grundlagen der Zahlentheorie*), 5. Auflage (Moskau—Leningrad, 1949), insb. S. 87, Beispiel 8.

(Eingegangen am 21. April 1953.)